

GeekBrains

Урок 5 Видео 1

Криптография

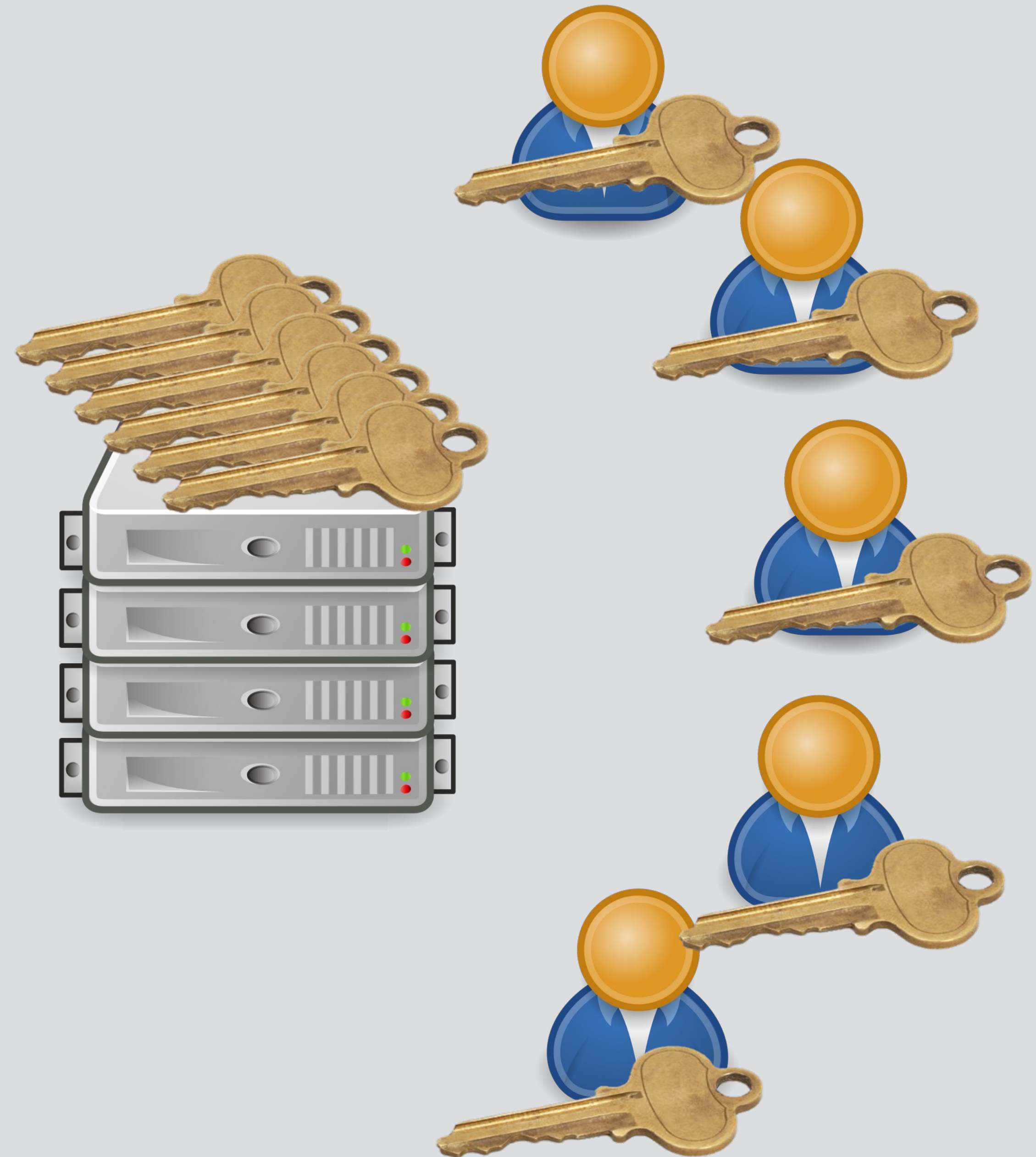
RSA

В этом видео

1. Асимметричная криптография
2. Шифрование с помощью RSA
3. Подпись с помощью RSA
4. Почему RSA не используется вместо блочных и потоковых шифров?

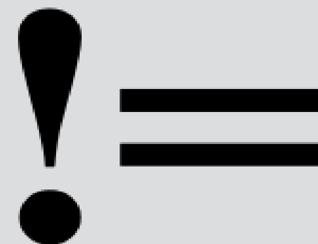
GeekBrains

Что делать, если нужно зашифрованное соединение с тысячами (и более) клиентов?



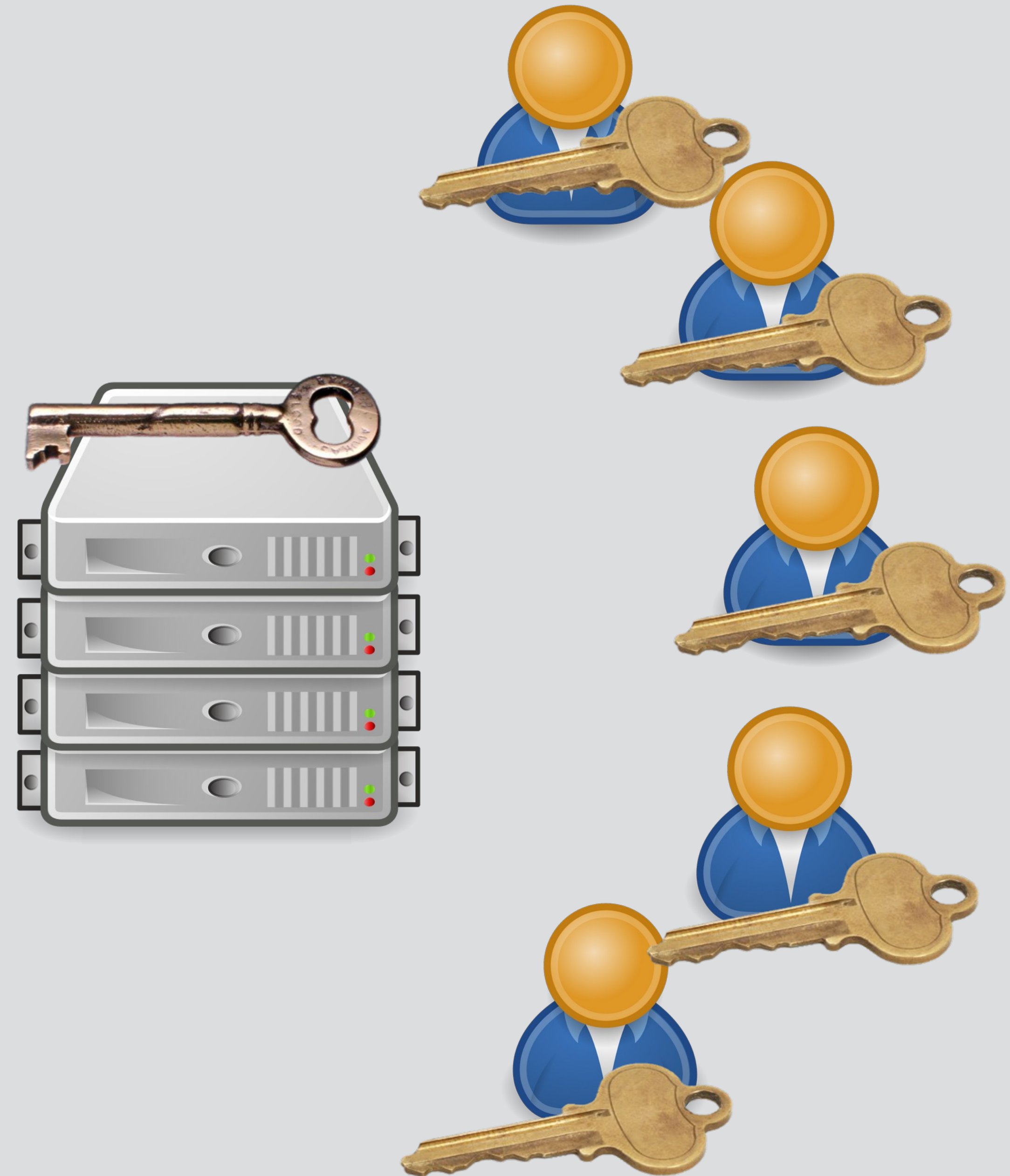
Асимметричная криптография — криптосистема, в которой шифрование и дешифрование происходит с помощью пары разных ключей (открытый и закрытый).





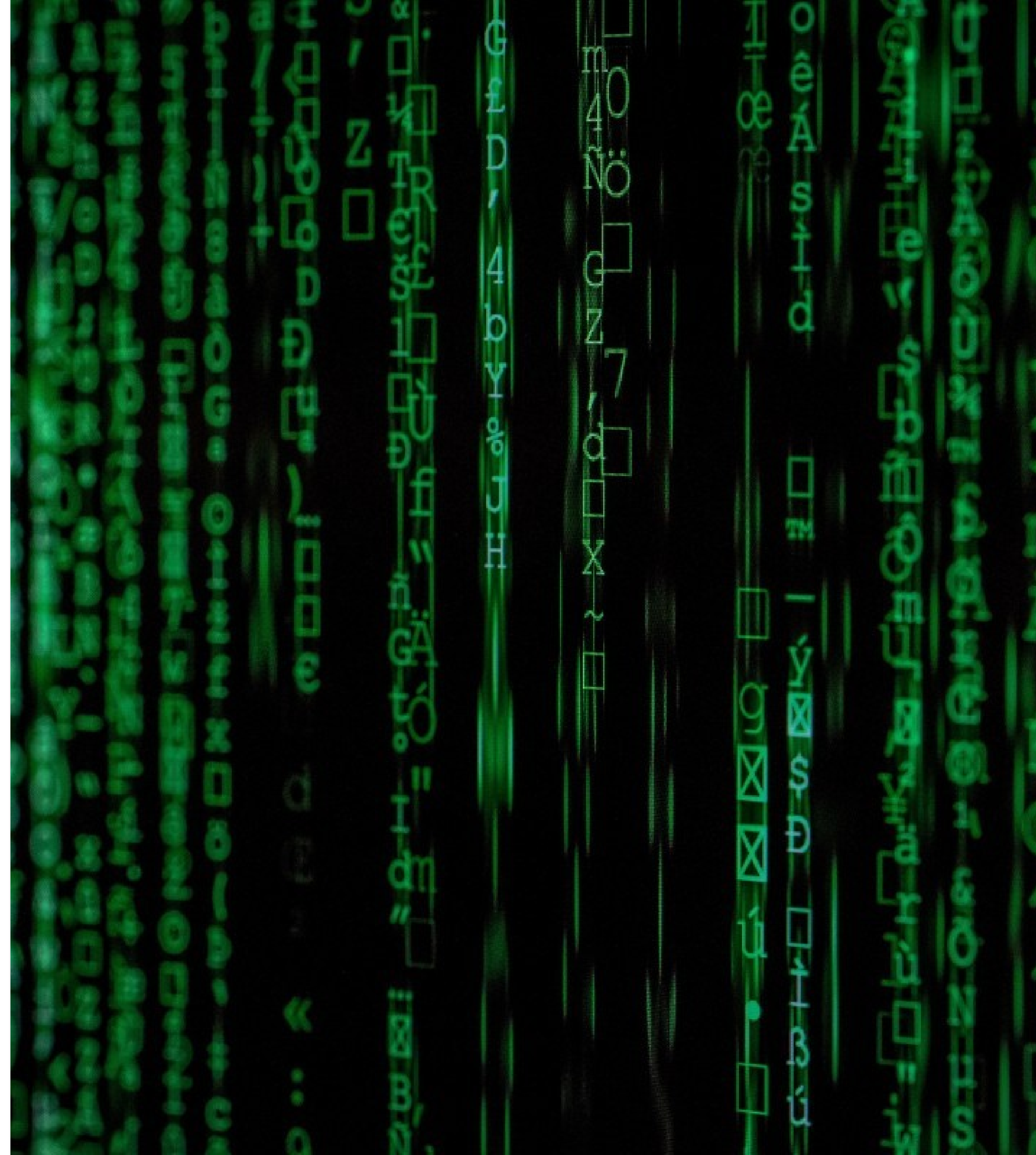


Асимметричная криптография — криптосистема, в которой шифрование и дешифрование происходит с помощью пары разных ключей (открытый и закрытый).



Шифрование RSA

Для шифрования с помощью RSA используется открытый ключ, а для расшифрования используется закрытый ключ



Подпись RSA

Для подписи с помощью RSA используется закрытый ключ, а для проверки подписи используется открытый ключ



Симметрия vs асимметрия

Главная причина, по которой асимметричная криптография не заменила симметричную — скорость вычислений



Итоги

1. Асимметричная криптография
2. Шифрование с помощью RSA
3. Подпись с помощью RSA
4. Сравнили симметричные шифры и RSA